Information Services Board Briefing Paper on Statewide Information Technology Policy Compliance

Prepared by Mary Lou Griffith, DIS/MOSTD, (360) 902-2978.

Description

ISB staff will review the status of agencies' certification compliance with IT policy and standards pertaining to Portfolio Management, Disaster Recovery/Business Resumption, and IT Security Program reviews.

Recommendations to the Board

ISB staff recommends that for non-compliant agencies the Board reduce delegated authority for information technology purchases by 25%. The Liaison to the Board will notify the non-compliant agencies. Staff also recommends that by the next scheduled ISB meeting the Board require non-compliant agencies to provide a specific date that they will be compliant. Finally, staff recommends that the Board delegate to the Liaison the authority to restore agencies' delegated authority upon certification that they are in compliance with the respective ISB policies and standards.

Status

The agencies' annual review letters were received by the ISB Liaison and have been tracked and logged. Agencies that responded represent more than 90% of the state IT expenditures. The results below are based on data collected through March 1, 2004.

IT Portfolio Management: Out of 121 agencies, 108 agencies' portfolios have been reviewed and updated. One agency indicated it was still completing its portfolio and requested an extension.

Disaster Recovery/Business Resumption: Of 121 agencies, 109 stated their disaster recovery/business resumption plans have been reviewed. One agency requested an extension, stating it is working on updating its plans, but is not completely finished.

Security: Of 121 agencies, 113 reported they have completed their security program development. One agency requested an extension to complete its security program and audit. One hundred and two agencies have reported their audit was performed.

Security Standards Enhancement: ISB staff and a team of security professionals from the Washington Computer Incident Response Center (WACIRC) will update the IT Security Standards. The update will clarify the interpretation of the standards and add new standards for patch management and remote access.

Issues

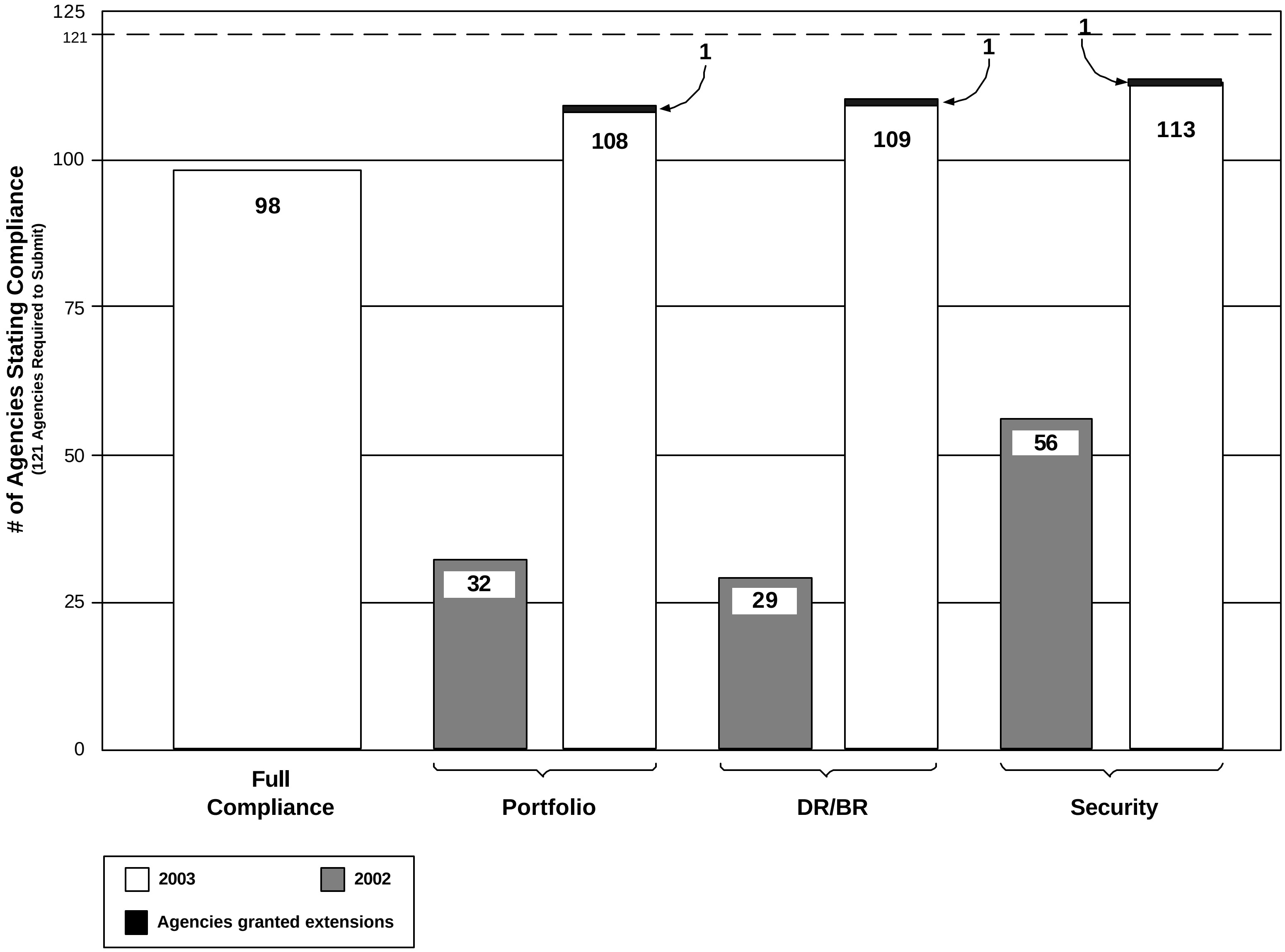
- Several agencies indicated the need to update their Disaster Recovery/Business Resumption Plans, but cite lack of resources (budget and/or staff) to do so.
- On-going support in the form of training and technical assistance is needed for small agency ISB policy compliance.
- Several agencies continue to assert that budget constraints affect their ability to provide adequate resources to comply with security policy requirements and the audit provision.

Background

The ISB policies direct agencies to review and update their IT Portfolio, Disaster Recovery/Business Resumption Plan and their IT Security Program annually. Each agency director is responsible for oversight of the agency's plans and programs and will confirm in writing annually by August 31st that the portfolio was reviewed and updated, the Disaster Recovery/Business Resumption Plans have been reviewed, updated, and tested and the IT Security Program has been developed, reviewed and updated.

Additionally, the IT Security policy requires agencies to conduct an IT security policy and standards compliance audit once every three years. The audit is a desk review of the documented agency security processes and procedures. The exceptions to the policy and standards are provided only to the agency following the audit. Knowledgeable parties independent of the agency's information technology unit, such as a state auditor, must perform the audit. Agencies must follow audit standards developed and published by the State Auditor. All agencies under the authority of the ISB were required to complete their initial compliance audit by October 6, 2003.

ISB IT Policy & Standards Compliance for 2002 and 2003


# of Agencies Stating Compliance
(121 Agencies Required to Submit)
Full Compliance
Portfolio
DR/BR
Security
Agencies granted extensions